Real Cryptographers are Mathematicians, Beware of Everyone Else

AusCERT 2012

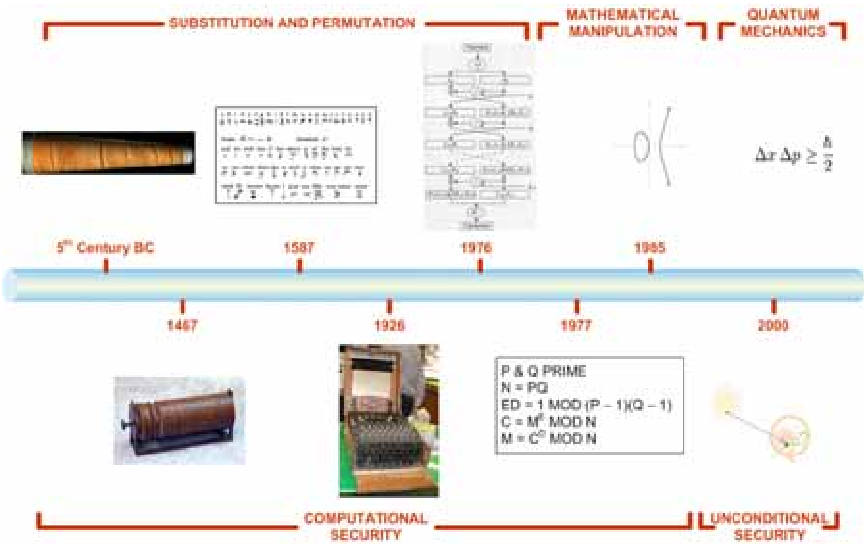
John Leiseboer, CTO

QuintessenceLabs Pty Ltd

Agenda

- **Background**
- **Introduction to Theory of Quantum Key Distribution**
- **Applied QKD**
- **Question Time**

A Brief History of Cryptography



Quantum Mechanics

- **Explains the behaviour of matter and its interactions with energy on the scale of atoms and atomic particles**
- **Particle-wave duality**
  - Subatomic particles can have both wave-like and particle-like properties
- **Uncertainty principle**
  - Certain pairs of physical properties, such as position and speed, cannot both be known to arbitrary precision
  - Heisenberg showed that the more precisely one of them is known, the less precisely the other can be known
- **Practical applications of quantum mechanics**
  - The laser, the transistor, the electron microscope, magnetic resonance imaging
  - The study of semiconductors led to the invention of the diode and the transistor, which are indispensable for modern electronics

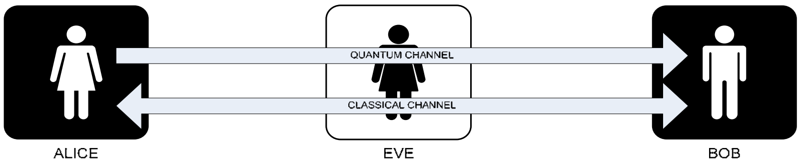
Encryption Systems Today

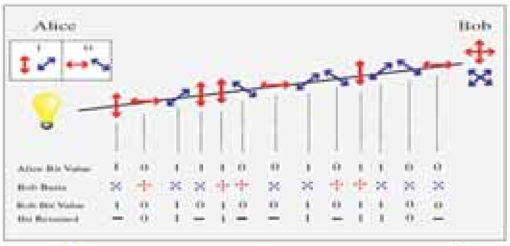
- **Security today is dependent on one or more assumptions**
  - **Efficient mathematical** attacks will never be feasible
  - **Computing resources** will never be sufficiently powerful for brute-force attacks
  - New technologies such as **quantum computers** will never be developed to sufficient scale
  - **Public Key Infrastructure** will always be secure from attack
  - **Trusted Third Parties** can always be trusted for authentication

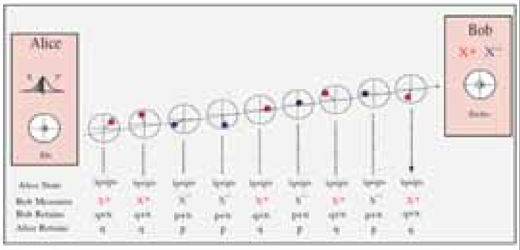
- **Long-lived data encrypted by conventional methods can be stored for future decryption**
  - Sovereign/criminal eavesdropping activity
  - **Such data at risk today**

INTRODUCTION TO THE THEORY

How QKD Works





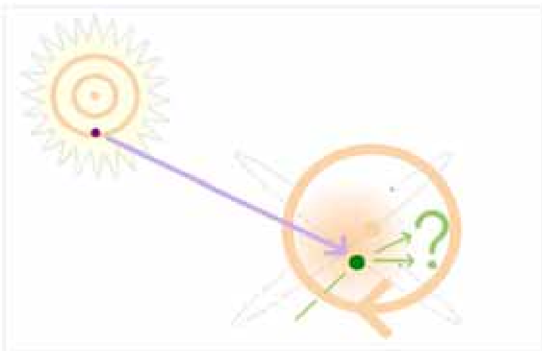


Discrete Variable

Continuous Variable

How is QKD Secure?

- **At a quantum level, certain pairs of variables cannot be known with arbitrary precision (e.g. position and momentum)**

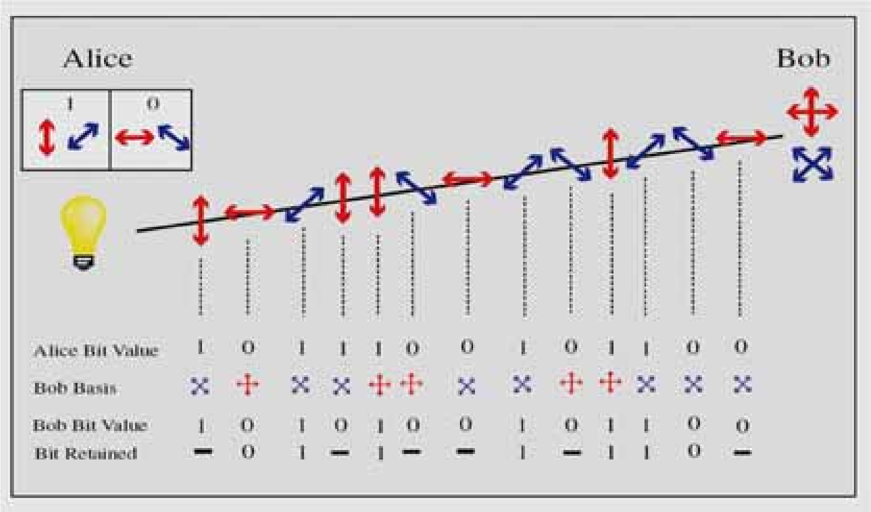


Heisenburg Uncertainty Principle

$$\Delta x \, \Delta p \geq \frac{\hbar}{2}$$

- **At the quantum level merely observing a particle will affect it e.g. light particles (photons) will bounce off particle, affecting it**

Single Photon QKD



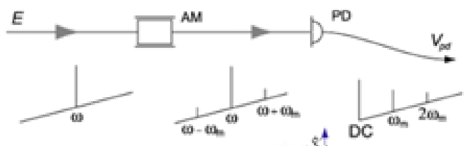
[Bennett and Brassard, *Proceedings IEEE.*, (1984)]

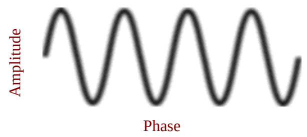
Discrete Variable Key Distribution

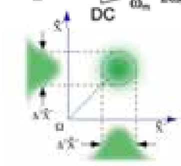
- **Alice generates a secret random bit sequence**
- **Alice encodes the sequence as quantum states on individual photons and sends it to Bob**
- **Alice and Bob sift the information**
  - Bob tells Alice what basis he used
  - Alice tells Bob if the basis he chose was correct or not
- **Alice and Bob reconcile errors and estimate Eve’s information**
- **Alice and Bob each perform privacy amplification**

“Bright Laser” QKD

- **Lasers are ideal for telecommunications**
- **Information can be encoded by varying the amplitude and the phase of a laser: AM and FM encoding**

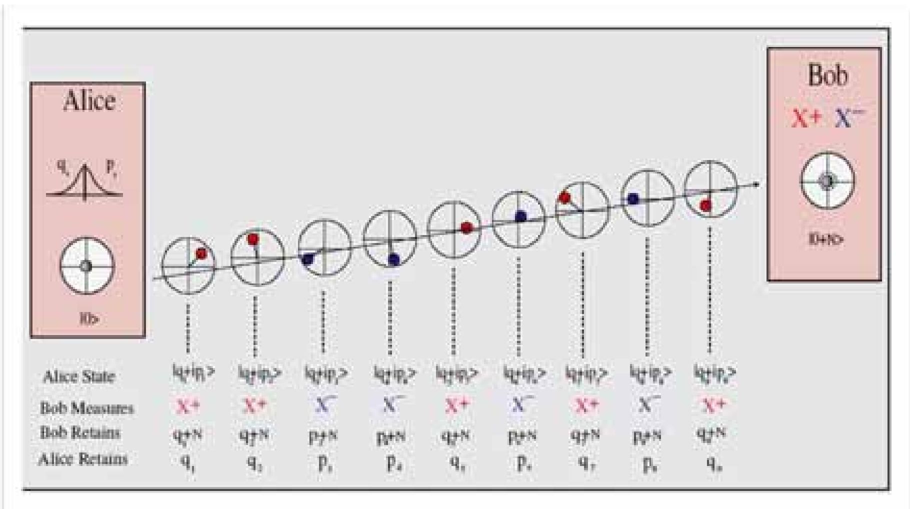






- **For a laser the amplitude and the phase of a laser beam cannot be simultaneously determined**
- **Quantum noise can be represented by a Ball and stick diagram**

Continuous Variable Analogue to BB84

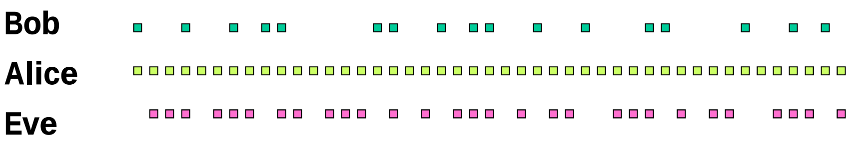


Continuous Variable Key Distribution

- **Alice generates a secret random bit sequence**
- **Alice encodes the sequence as quantum states on a laser beam and sends it to Bob**
- **Alice and Bob post select the information**
  - Bob tells Alice which bits he’s keeping
- **Alice and Bob reconcile errors and estimate Eve’s information**
- **Alice and Bob each perform privacy amplification**

Necessary Ingredients for QKD

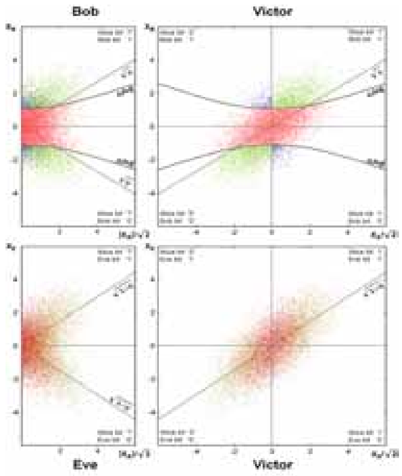
- **We only need two things**
- **Differential correlations**
  - Alice and Bob share different information to everyone else.



  - No-cloning theorem always guarantees this!
- **Known bounds**
  - Heisenberg uncertainty, no-cloning limit, Shannon entropy, etc.
  - There exist classical information protocols to distil secret key, reconcile data, and amplify privacy remotely.

Post Selection

- **Bob discards all the states for which he estimates he has less information than Eve (red).**
- **Eve has no control on that process and is left with less information.**



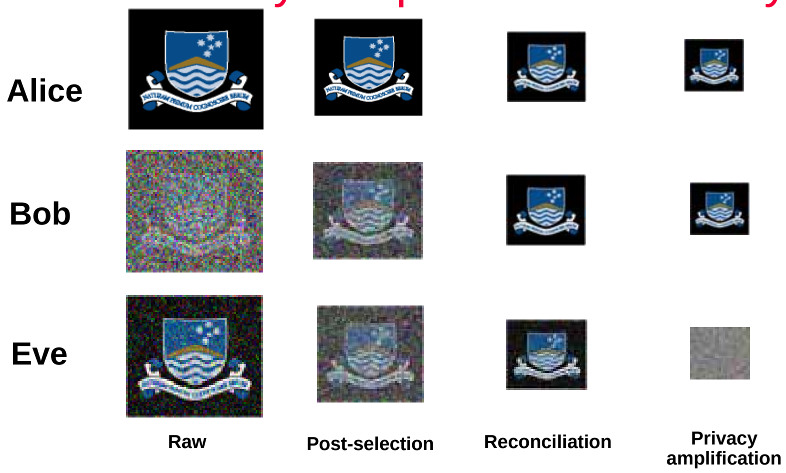
Privacy Amplification

$$\left[(1/0)x^{110503}+(1/0)x^{110502}+\ldots+(1/0)x+(1/0)\right]\times\left[r_{11503}x^{110503}+\ldots+r_0\right]$$

$$\mathrm{mod}\left[x^{110503}+x^{5011}+1\right]$$

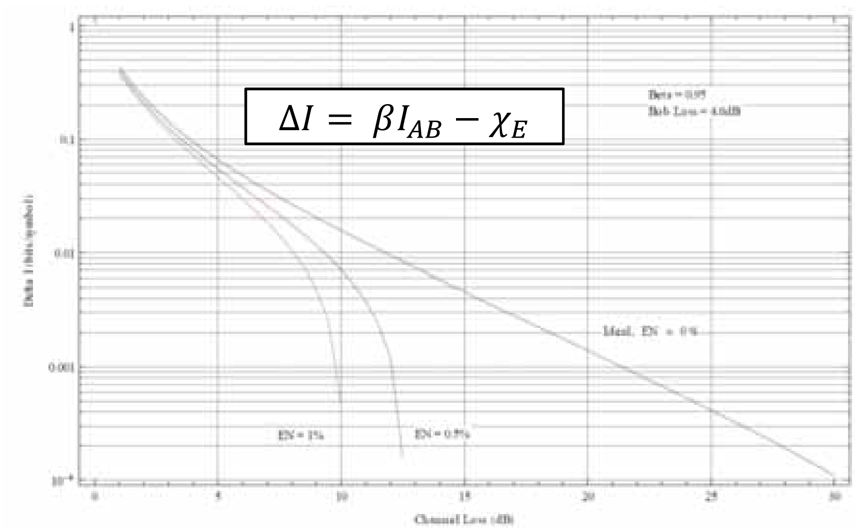
$$\left[f_{110503}x^{110503}+f_{110502}x^{110502}+\ldots+f_1x+f_0\right]$$

Summary: Steps to a Secret Key



Link Loss	Raw	Ch. Ch.	Post Sel.	Error Rec.	Priv. Amp.
54% (~3 dB)	100%	50%	33%	17%	1.3%
90% (10 dB)	100%	50%	0.2%	0.03%	0.003%

Performance



The Future

- **Remove Excess Noise**
  - Provisional patent drafted for a method of post selection to create a virtual channel with zero excess noise from a channel affected by excess noise
  - Fixes distance issue
- **Reconciliation Efficiency**
  - FEC using LDPC can improve β better than linearly
  - Values of β approaching 0.95 are theoretically possible
- **Brute Force**
  - Higher transmission rate, more sidebands, more channels
  - See next slide

Brute Force Scaling

Number DWDM Channels	1	2	4	8	16	32
Insertion Loss of DWDM components	0 dB	<=1dB	<=1dB	<=3.5dB	<=4.5	<=5.4
Net Raw Key Rate	3.2 Gbit/s	6.4 Gbit/s	12.8 Gbit/s	25.6 Gbit/s	51.2 Gbit/s	102 Gbit/s
Final Secret Key Rate @ 5dB loss (~25 km)	192 Mbit/s	340 Mbit/s	678 Mbit/s	768 Mbit/s	1.2 Gbit/s	1.8 Gbit/s
Final Secret Key Rate @ 10dB loss (~50 km)	48 Mbit/s	85 Mbit/s	170 Mbit/s	180 Mbit/s	277 Mbit/s	451 Mbit/s
Final Secret Key Rate @ 25dB loss (~125 km)	1.3 Mbit/s	2.0 Mbit/s	3.8 Mbit/s	4.6 Mbit/s	7.5 Mbit/s	12.3 Mbit/s

APPLIED QKD

Application of QKD

- Embeddable KM libraries enforcing security policy
- Link and network encryption
- One-time pad cipher support
- Third party device and application support

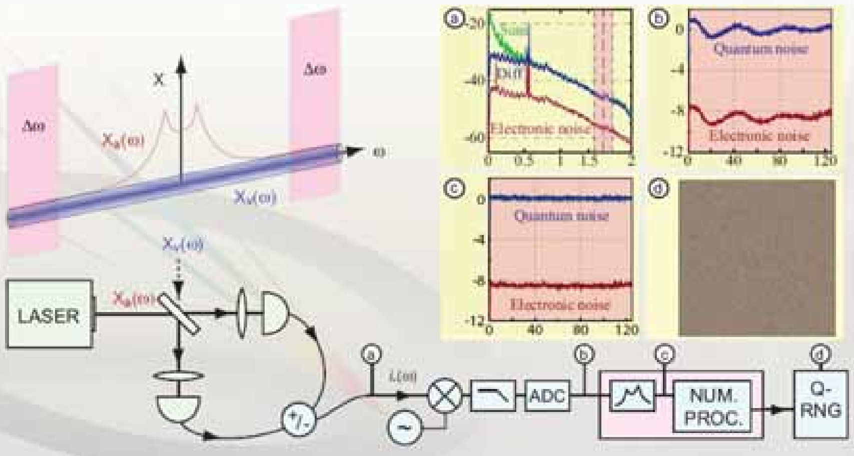
- Secure key lifecycle management
- Cryptographic policy and control
- Separation of duty
- Authentication, logging and audit
- OASIS KMIP interface

- Continuous variable QKD
- Fibre optic and free space (planned) media
- Optional implementation levels to suit environment

- Quantum entropy source
- Optical and electronic hardware true RNG
- Very high speed

Quantum Entropy Source

Implementation



2 Gbit/s achieved

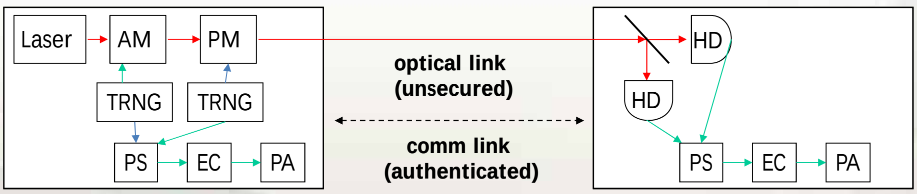
Passes NIST & Dieharder tests

Quantum Key Distribution

Optical layer

Alice

Bob



- **Alice**
  - Generates string of random data bits (TRNG)
  - Prepares & transmits displaced coherent states (AM & PM)
- **Bob**
  - Measures **both** amplitude and phase quadratures (2xHD)
- **Alice & Bob**
  - Determine Eve's information (random 50% of data)
  - Post-selection (PS)
  - Error correction (EC)
  - Privacy amplification (PA)

Key Management

Quantum Key Manager

quintessencelabs

- **Manages cryptographic key and related material**
  - Distributed, information-theoretic secure key generation
  - Centralised security policy management
  - Cryptographic key lifecycle management
- **Provides secure key distribution**
  - Authenticates access requests
  - Logs access requests
- **Is simple to use**
  - OASIS KMIP interface
  - Vendor neutral
- **Lowers cost**
- **Improves security**

OASIS KMIP TC Members

American Express
Axway Software
CA Technologies
Credant Technologies, Inc.
Cryptsoft Pty Ltd.
Election Systems & Software
EMC
Emulex Corporation
EURECOM
Freescale Semiconductor, Inc.
Hewlett-Packard
IBM
IECA, Inc.
Lexmark International Inc.
M.I.T.

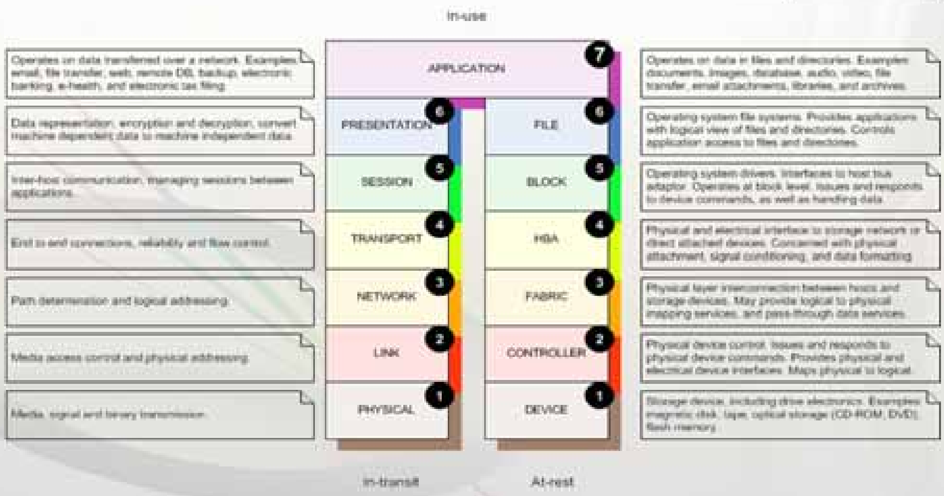
OASIS KMIP TC Members

Mitre Corporation
National Security Agency
NetApp
NIST
Oracle
PrimeKey Solutions AB
Quantum Corporation
QuintessenceLabs Pty Ltd.
Red Hat
SafeNet, Inc.
Skyworth TTG Holdings Limited
Symantec Corp.
Target Corporation
Thales e-Security
UNH Interoperability Laboratory
Venafi, Inc.
Voltage Security
Vormetric, Inc.

Information Protection

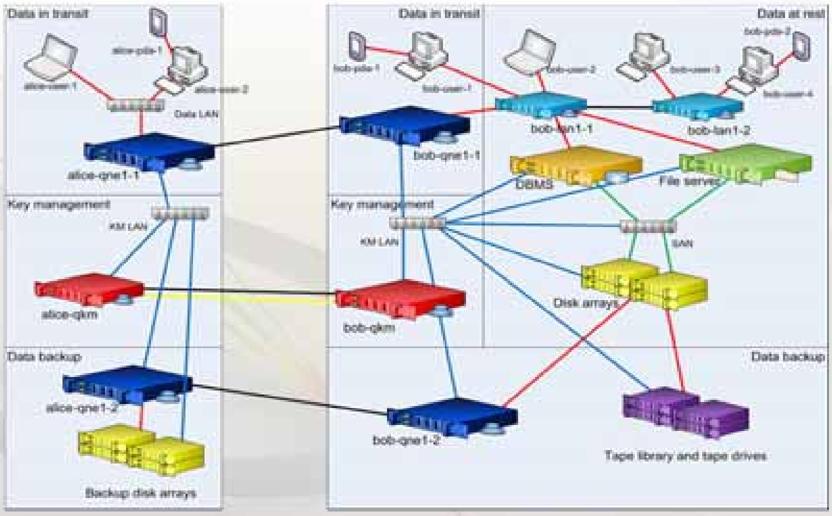
Data ARITIU Model

quintessencelabs



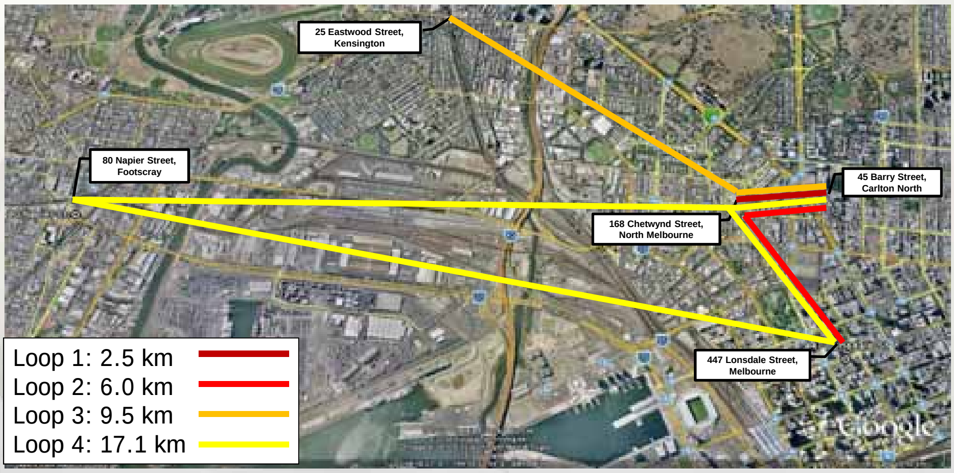
Deployment

Heterogeneous IT Environment



Telstra Pilot

November, 2010



Proposed Deployment

NASA/JPL - 2012

- **Prototype unconditionally secure communications network, spanning fibre and free space links**
- **Phased project**
  - Terrestrial fibre
    - NASA Ames to JPL Pasadena
  - Terrestrial free space
  - Ground to aircraft
  - Ground to satellite

Questions?

John Leiseboer

CTO, QuintessenceLabs Pty Ltd

jl@quintessencelabs.com